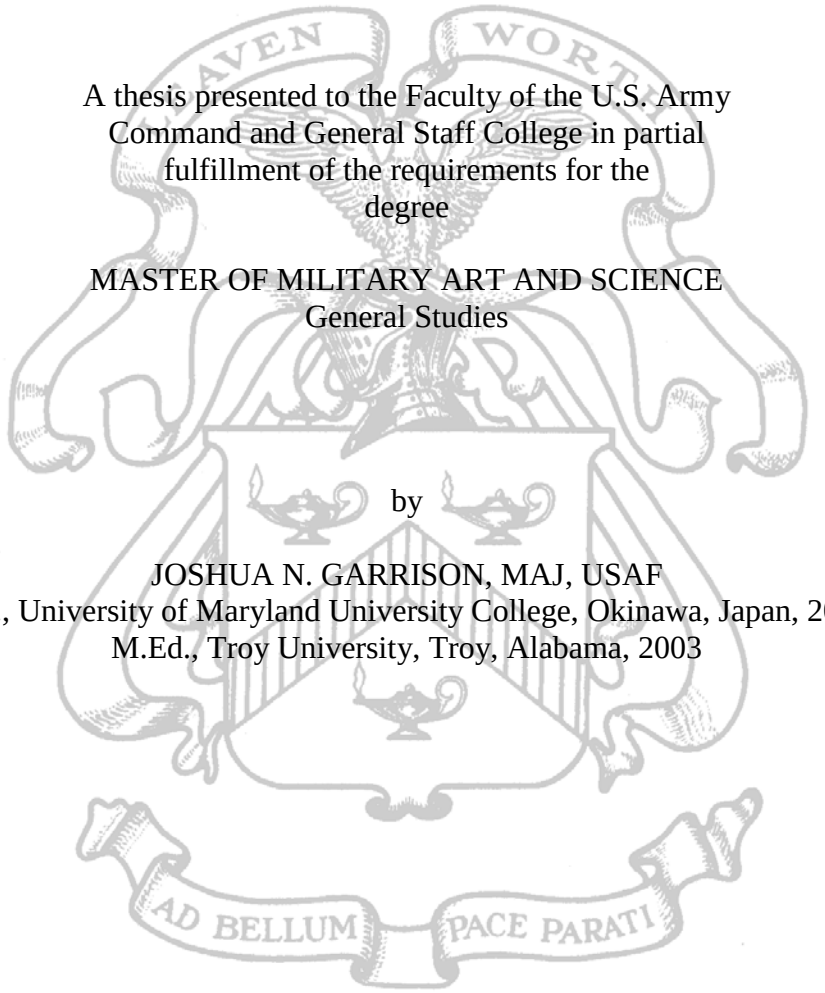
FUTURE OF UNITED STATES CYBER: EXAMINING THE PAST TO POSTURE THE FUTURE

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

JOSHUA N. GARRISON, MAJ, USAF
B.A., University of Maryland University College, Okinawa, Japan, 2000
M.Ed., Troy University, Troy, Alabama, 2003



Fort Leavenworth, Kansas
2013-02

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-12-2013	Master's Thesis	FEB 2013 – DEC 2013

4. TITLE AND SUBTITLE
Future of United States Cyber: Examining the Past to Posture the Future

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Joshua N. Garrison, Major, USAF

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The United States (U.S.) and its allies face an ever growing cyber threat. The emergence of the cyber domain has brought cyber threats and vulnerabilities to the forefront of U.S. national security. The ability to effectively operate defensively and offensively in cyberspace is crucial to U.S. military forces. Considering cyber is still relatively in its infancy, we can learn a lot from previous experiences in adopting a new domain for military operations. The rise of air power during the first half of the 20th century and the ascension of space power during the second half of the 20th century provides a backdrop for comparing against current cyber policies, strategies, and regulations.

15. SUBJECT TERMS
Cyber, Offensive, Defensive, Operations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	66	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Joshua N. Garrison

Thesis Title: Future of United States Cyber: Examining the Past to Posture the Future

Approved by:

_____, Thesis Committee Chair
Kenneth C. Rich, Ph.D.

_____, Member
Loye W. Gau, M.A.

_____, Member
Steven Wiegers, M.S.

Accepted this 13th day of December 2013 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

FUTURE OF UNITED STATES CYBER: EXAMINING THE PAST TO POSTURE THE FUTURE, Major Joshua N. Garrison, 66 pages

The United States (U.S.) and its allies face an ever growing cyber threat. The emergence of the cyber domain has brought cyber threats and vulnerabilities to the forefront of U.S. national security. The ability to effectively operate defensively and offensively in cyberspace is crucial to U.S. military forces. Considering cyber is still relatively in its infancy, we can learn a lot from previous experiences in adopting a new domain for military operations. The rise of air power during the first half of the 20th century and the ascension of space power during the second half of the 20th century provides a backdrop for comparing against current cyber policies, strategies, and regulations.

ACKNOWLEDGMENTS

This thesis and my success at Command and General Staff College would not have been possible without the amazing support and sacrifice of my wife, Lachanda, and our children, Jashaun and Jasmine. They patiently accommodated my schedule and kept me grounded through a challenging year at Command and General Staff College.

I was extremely blessed to have the best staff group instructors at the Command and General Staff College: Mr. Loye Gau, MAJ Kenneth Rich, Mr. Steven Wiegers, Dr. Bill McCollum, Mr. Jeffrey Holcomb, LTC Andrew Lanier, and Dr. Alexander Bielakowski. Their expert instruction and support made this year especially rewarding, and I found their classes influencing numerous aspects of my research. Additionally, all of the members of Staff Group 2D were instrumental in my success while attending Command and General Staff College. Their expertise and friendship were second to none.

A special thanks to MAJ Kenneth Rich, Mr. Loye Gau, and Mr. Steven Wiegers for serving as my committee members. Their guidance was significant in developing my thesis and keeping me focused with my research. I cannot thank them enough for their support, patience, and diligence in reading numerous versions of my thesis.

TABLE OF CONTENTS

Page

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

> America must also face the rapidly growing threat from cyber-attacks. Now, we know hackers steal people's identities and infiltrate private emails. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.[1]
>
> — President Barack Obama, 2013 State of the Union Address

Cyberspace is the fifth warfare domain after land, air, sea, and space. It is the newest domain and is unique to the other four domains in that it is entirely manmade. Although, it can be argued that the space domain is only relevant due to manmade technology making cyberspace a variation of space. However, the construct and operations between space and cyberspace are completely different, as cyberspace is the global domain within the information environment. Cyberspace includes the interdependent network of information technology infrastructures and resident data (i.e. the Internet, telecommunications networks, computer systems, and embedded processors and controllers). Cyberspace consists of three separate layers, the physical network, the logical network, and the cyber-persona network.[2]

The physical network layer encompasses the geographic elements and the physical network elements in which data travels. The locations in air, land, sea, and space

---

[1]The White House, "Remarks by the President in the State of the Union Address," 12 February 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address (accessed 30 March 2013).

[2]Joint Education and Doctrine, "Joint Publication 3-12, Cyberspace Operations-Unclassified Excerpts," *Joint Doctrine Update* 8, no. 2 (April 2013), 1.

where components of the network exist make up the geographic component. The hardware, system software, and infrastructure that sustain the network and physical connectors involve the physical network.[3]

The logical network layer represents how the intricate communication of information flows within the physical network. It comprises the components of the network that are interconnected together in a manner that is abstracted from the physical network.[4] An analogy is using the linking of railways to various train stations to symbolize the physical network and the trains traveling to the stations represent the logical section of the network.

The cyber-persona layer is a sophisticated conception of the logical network and employs policies relevant in the logical network to create a digital portrayal of a person or entity in cyberspace. Essentially, the cyber-persona layer comprises the individuals using the network. This layer can associate directly to an entity or actual individual containing various company or personal data.[5]

[3]Ibid., 1.

[4]Ibid., 2.

[5]Ibid.

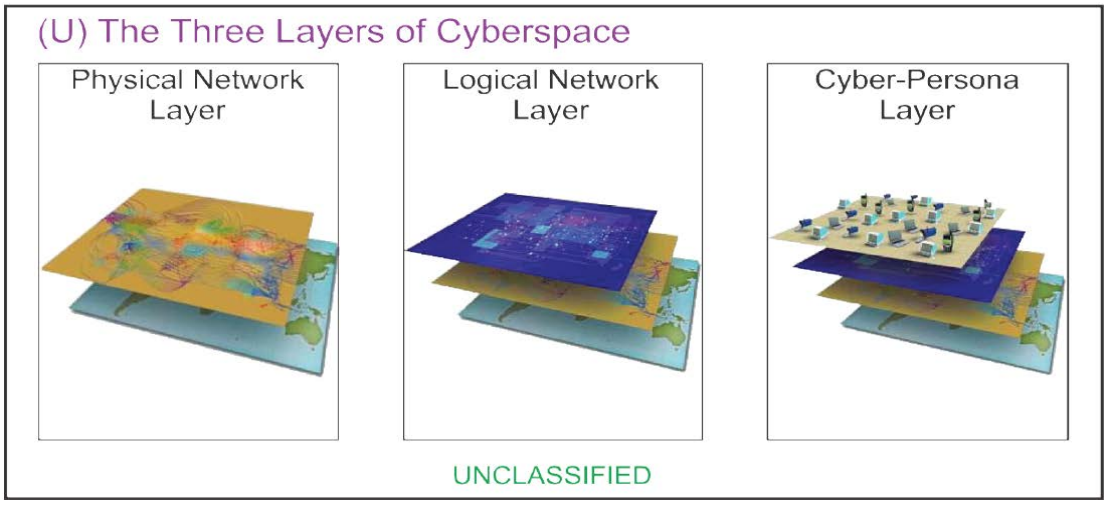


Figure 1. A Graphical Representation of the Three Layers of Cyberspace

Source: Joint Education and Doctrine, "Joint Publication 3-12, Cyberspace Operations-Unclassified Excerpts," *Joint Doctrine Update* 8, no. 2 (April 2013), 2.

It is also important to introduce and describe the information environment in which the cyberspace domain resides. The information environment is the accumulation of people, systems, and institutions that gather, administer, distribute, and—or take action on information. This environment consists of the physical, informational, and cognitive dimensions.[6]

The physical dimension includes command and control systems, key leaders, and supporting infrastructure that allow people and institutions to produce desired effects. The communications networks that link physical interfaces (i.e. tablets, smart phones, people, command and control facilities, etc.) reside in the physical dimension. This dimension is not unique to the military or nations with sophisticated systems and

[6]Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (Washington, DC: Government Printing Office, November 2012).

established protocols. It is a decentralized network linked across national, geographic, and economic boundaries.[7]

The informational dimension indicates how and where information is gathered, processed, distributed, and safeguarded. Command and control of military forces is implemented in this dimension and where the commander's intent is communicated. Actions taken in this dimension directly affect the content and distribution of information.[8]

The cognitive dimension incorporates the mental aspect of sending, receiving, and responding to or acting on information. This dimension represents the most significant element of the information environment and portrays how people process, perceive, and judge information. Cultural beliefs, customs, weaknesses, emotions, motivations, education, ideologies, mental health, and other differentiating factors vary from individual to individual and group to group. It is crucial to define these factors in any environment in order to figure out the best way to influence leaders and shape the desired outcomes.[9]

The complex dimensions in the information environment make it very challenging to integrate cyberspace operations. These challenges include overlapping efforts and responsibilities between the military and the private sector along with foreign rules,

[7]Ibid.

[8]Ibid.

[9]Ibid.

regulations, and rights to cyberspace. Threats in cyberspace consist of nation states, criminal organizations, and terrorist groups.[10]

Given the challenges of paving the way ahead for operating in a relatively new cyber domain, can the United States (U.S.) learn anything from the failures and successes during the emergence of air and space power that are relevant to the cyber environment today, in order to avoid making similar mistakes and exploit past achievements where possible? What events led to the establishment of the U.S. Air Force? Why was a separate U.S. Space Force not established? What is the cyber domain? What are the current and potential future cyber threats and capabilities? What is the Department of Defense currently doing to combat these threats? Do the current military state of affairs in cyber compare to the issues and challenges faced in the air and space domain? What options are available for the Department of Defense to consider in the coming years, in order to effectively operate offensively and defensively in cyberspace?

Assumptions

For purposes of this research study, a key assumption is that the cyber domain will continue to exist, threats will persist into the future, and the military will play a major role in cyber operations. Additionally, it is assumed that past air and space power experiences are similar enough to current cyber events that warrant a research study. This assumption serves as a baseline for comparative analysis of the emergence of the air, space, and cyberspace domains for military operations and recommended options presented for the future of cyber operations.

[10]Ibid.

Definitions

Cyber Attack: non-lethal offensive operation intended to create physical effects or manipulate, disrupt, or delete data.

Cyber Espionage: act of stealing information from individuals, competitors, rivals, groups, governments, and enemies for personal, economic, political, or military advantage using methods on the Internet, networks, or individual computers.

Denial of Service: an attempt to make a computer or network resource unavailable to its intended customers.

Limitations

This thesis is written at the unclassified level, although more in-depth information is available at the classified level. Offensive and defensive cyber concepts and capabilities are relatively new and the world is still determining boundaries, guidelines, and laws for operating within cyberspace. In order to provide increased awareness and discussion of how the Department of Defense addresses cyber threats, this research study will only include open source and unclassified viewpoints of cyber strategies and regulations.

Delimitations

In determining whether there are any lessons learned from experiences in the air and space domains, this research study focuses on the first half of the 20th century for the air domain, with the first manned flight in 1903 to the establishment of the U.S. Air Force in 1947 and focuses on the second half of the 20th century for the space domain, with the start of the space race through the first Gulf War in 1991. Additionally, since the

significance of cyber for military operations is still relatively new, this research study focuses primarily on the 21st century for the cyber domain.

Summary

The U.S. and its allies face an ever growing cyber threat. This thesis focuses on identifying positive and negative lessons learned during the emergence of air and space power, to determine applicability to today's challenges with the emergence of cyber power. This study highlights the challenges the air and space community faced initially and how they overcame the challenges. Additionally, the current U.S. cyber posture along with potential threats and vulnerabilities to the military and civilian sector will be examined. In order to accomplish these objectives, this study examines the emergence of air and space power and compares it to current U.S. cyber policies, strategies, and regulations. In describing the current U.S. cyber posture, this study highlights the similarities between cyber and the initial air and space policy and organization. Additionally, a growing disconnect between government and civilian leaders on the best ways to address the mounting cyber threat may potentially impede U.S. progress of necessary defensive and offensive operations in cyber. The study concludes with providing options for how the Department of Defense can organize cyber operations, in order to adequately manage current and potential future cyber threats.

CHAPTER 2

LITERATURE REVIEW

Since the cyber domain is still in its infancy, exploring the historical military background of the air and space domains reveals the complexity of understanding a new domain. Many of the experiences the air and space domains encountered initially are similar and relevant to the cyber environment today. Furthermore, the Air Force was established less than 70 years ago and the space domain became prominent since then as well, making air and space significance a relatively recent period in history. First, I will provide a historical background for the rise of air power during the first half of the 20th century, then transition to the ascension of space power during the second half of the 20th century, and finally cover the emergence of cyber power during the 21st century.

The Rise of Air Power

From the beginning of military aviation in the U.S., the idea of a separate Air Force existed in the military, Congress, and the civilian sector. Two questions survived throughout the rise of air power. Should aviation be a separate department like the Department of War and the Department of the Navy? Should aviation be matched with sea and ground forces under a department of national defense? Starting in 1916, more than 50 bills were introduced in Congress over three decades calling for a separate department of aviation or a coequal under a department of national defense. Multiple studies were conducted throughout the rise of air power to determine the feasibility of

separating aviation that produced recommendations recognizing the potential of aeronautics.[11]

Air warfare has been evident since the bow and arrow was used in combat but manned air combat did not occur until the last century. With the success of the Wright Brothers at Kitty Hawk, North Carolina in 1903, the idea of man achieving powered flight became a reality. Prior to 1903, hot air balloons were used during several American conflicts in the 1800s to include the Civil War but were primarily used for observation and reconnaissance.[12]

During the onset of World War I, air power was also predominately used for reconnaissance. The Allies did not execute direct air power against enemy forces using guns and bombs until two months after the war started. Even the U.S. was ill prepared to support aviation war efforts upon entering the war in 1917. With only 56 pilots and less than 250 airplanes, the U.S. fell tremendously short of the Allied recommended 4,500 airplanes and 5,000 pilots. By the time the war ended in 1918, the U.S. produced 11,754 airplanes and the Army established eight ground schools and 27 flying schools, with 35 advanced flying schools available in Europe.[13]

The effectiveness of offensive and defensive operations during World War I proved the importance of air power and the necessity for an independent strategic Air

---

[11]Alfred Goldberg, *A History of the United States Air Force 1907-1957* (Princeton: D. Van Nostrand Company, 1957), 99.

[12]Chester Hearn, *Air Force: An Illustrated History* (Minneapolis: Zenith Press, 2008), 11.

[13]Stephen L. McFarland, *A Concise History of the U.S. Air Force* (Washington, DC: Air Force History and Museums Program, 1997), 4.

Force. However, the U.S. Army and the U.S. Navy still considered air power as a supporting weapon for the land and sea domains respectively in the form of close air support, interdiction, reconnaissance, and air superiority above the battlefield. An evaluation on the lessons of World War I concluded the following, "Nothing so far brought out in the war shows that aerial activities can be carried on, independently of ground forces, to such an extent as to affect materially the conduct of the war as a whole."[14]

Widespread concurrence of the evaluation hindered efforts of an independent Air Force mainly due to the lack of air capability. The best bomber in the U.S. Army inventory following World War I, the French built Breguet, ranged 300 miles with a top speed of 100 miles per hour.[15] This presents a huge limitation in capability required for strategic bombing. From 1919 to 1926, continuous improvements in technology increased the range, speed, and reliability for strategic bombing. However, Army leadership still viewed air power as a tactical asset in support of the armed forces land and sea components.[16]

In October of 1924, following claims that Air Service officers were inappropriately favoring certain aircraft manufactures over others, the Lampert Committee was formed to investigate the accusations. Additionally, the Lampert Committee included other aviation innovations in the investigation which included the

[14]Ibid., 13.

[15]Ibid.

[16]Ibid.

need for an independent air service.[17] A vocal proponent of strategic bombing, Brigadier General Billy Mitchell, testified to the committee that the correct use of air power could destroy key transportation avenues, agricultural regions, and seaports before land and sea forces even arrive to the battlefield. Moreover, Mitchell heavily criticized the Navy and War Department's lack of air power understanding and continued prevention of a separate air service. For his actions, Mitchell was not reappointed to his position as the Assistant Chief of Air Service but instead was reassigned to Fort Sam Houston, Texas and returned to his permanent rank of Colonel.[18]

While in Texas, Mitchell continued his air power campaign in the media that eventually led to his court martial.[19] However, his insight brought air power capability to the forefront even further. After strategically waiting for the right moment, President Calvin Coolidge commissioned the Morrow Board to investigate Mitchell's air power claims. The Morrow Board was widely recognized as a fair and just approach to settle the air debate but Coolidge expected favorable results against a separate air service.[20] Following the testimony of 99 witnesses, most of them aviators to include an unsuccessful ploy by Mitchell, the Morrow Board determined that the U.S. was under no danger from aerial attack and dismissed the notion that strategic bombing could have an

[17]James P. Tate, *The Army and Its Air Corps: Army Policy toward Aviation, 1919-1941* (Maxwell Air Force Base: Air University Press, 1998), 35.

[18]Ibid., 36-38.

[19]Ibid., 40.

[20]Ibid.

effect on the will of opposing forces. Furthermore, the Morrow Board concluded that there should not be a Department of National Defense or a separate air service.[21]

However, two weeks following the release of the Morrow report, the Lampert Committee released its report which included recommendations for establishing a Department of National Defense, appointing air service representatives on the Army General Staff and Navy General Board, and also included many of Mitchell's ideas on air power.[22] Over several months, a political debate between Morrow and Lampert proponents ensued with both sides eventually coming to a compromise. This compromise led Congress in making the first step toward an independent Air Force by establishing the U.S. Army Air Corps on 2 July 1926. This act made the Army Air Corps an offensive force equivalent to the infantry and artillery.[23]

Leading into the 1930s, further technological improvements continued with the B-17 achieving high altitudes and a top speed of 252 miles per hour. The B-17 could outrun the fastest fighter of the day, the P-26, by up to 18 miles per hour leading the focus of Army Air Corps leaders towards strategic bombing. Thus, strategic bombing became the primary focus of expanding air power for senior aviation leaders.[24] As a result, Congress approved the first designated American Air Force, the General Headquarters Air Force, on 1 March 1935.

---

[21]Ibid., 41.

[22]Ibid., 45.

[23]Ibid., 47.

[24]McFarland, 18.

The General Headquarters Air Force directed all offensive aviation in the nine corps areas of the U.S. and managed the Army's organization, training, and operations for aviation.[25] However, instead of being controlled by the Army Air Corps, the General Headquarters Air Force fell under the Army Chief of Staff during peacetime and under the commander of field forces during wartime. This was due to the ongoing conflicting beliefs in the senior military ranks regarding independence of air power. For example, Brigadier General Frank Andrews, Commander of the General Headquarters Air Force, believed in a separate Air Force, whereas Major General Oscar Westover, Chief of the Air Corps, opposed air separation throughout his career due to his belief of the logistical support advantages air power presented to the Army.[26] This separation of authority was never supported by Air Corps leaders and eventually reorganized. The General Headquarters Air Force remained separated from the Army Air Corps until March of 1939.[27]

One issue with the advancement of air power is the Army continued to focus on tactical aviation to support soldiers on the ground instead of the strategic possibilities. In 1936, a committee chaired by Brigadier General Hap Arnold studied the best way to develop a "Balanced Air Program." The committee determined the Army needed only 1,399 airplanes in 1936 with an increase to 2,708 by 1941. However, the combination of the B-17 advancement and Adolf Hitler's air power success during the Sudetenland-

---

[25]Ibid., 19.

[26]Dik Daso, "Origins of Airpower," *Airpower Journal* 11, no. 3 (Fall, 1997): 94-113, http://search.proquest.com/docview/217772366?accountid=28992 (accessed 1 November 2013).

[27]McFarland, 19.

Czechoslovakia crisis of 1938 persuaded President Franklin Roosevelt to purchase 5,500 aircraft, in order to expand Air Force assets and capabilities.[28]

Upon Germany's invasion of Poland in 1939, the Air Corps employed roughly 26,000 airmen and 23 B-17s made up the heavy bomber force. After France fell to Germany in 1940, Roosevelt determined the Air Corps needed 50,000 aircraft and 54 combat groups leading Congress to allocate $2 billion towards expanding both the tactical and strategic air forces.[29] The amount of aircraft required and the scope of strategic focus began to exceed the span of control for the Army.

After taking command of the Army Air Corps in 1938, General Arnold recognized the military engineer's inability to create advanced aviation technology and realized that civilian expertise was the only way to guarantee the Army Air Corps had the best and most current technology around. Arnold sought expertise from the civilian sector recruiting expert scientists from academic institutions. Still, some expert scientists in the private sector could not see the potential in advanced aviation calling the study of jet propulsion fantasy and a waste of time for any serious scientists or engineers.[30] Furthermore, these same expert scientists believed that the military, other than production, should be excluded from aviation research and development. However, Arnold believed that without military input, the civilian sector would determine air power doctrine and policy.[31]

---

[28]Daso, 94-113.

[29]McFarland, 20.

[30]Daso, 94-113.

[31]Ibid.

Fortunately, Arnold was able to employ a circle of scientists and engineers dedicated to advancing U.S. air power. Under much criticism, he predicted that future aircraft would reach speeds in excess of 1,000 miles per hour. In the military realm, Arnold still found it difficult to convince opponents of air power independence of the potential, capabilities, and relevancy in warfare.[32]

Air power legitimacy continued to move forward with the establishment of the U.S. Army Air Forces in June of 1941 but the Japanese surprise attack at Pearl Harbor on 7 December 1941 revealed the U.S. Army Air Forces were still unprepared for war. Even though Admiral Husband Kimmel, Commander in Chief of the Pacific Fleet, put the fleet on first-class alert, Army Lieutenant General Walter Short failed to recognize the potential air threat and did not notify his air commander to adequately prepare for an air attack.[33] Short's misgivings partially came from the war plans officer of the Pacific Fleet who reported that the Japanese would never attack Pearl Harbor by air. Although an adequately prepared air defense would not have prevented the attack on Pearl Harbor, the 231 U.S. available aircraft in the area could have significantly mitigated the amount of losses sustained.[34]

Altogether, the U.S. air power could not prevent the Japanese from destroying 66 percent of the aviation assets at Pearl Harbor and 277 aircraft the following day near the Philippines to include 35 B-17s. Within a few months, the War Department reorganized with considerations towards a separate independent Air Force. However, senior leaders

[32]Ibid.

[33]Goldberg, 54-55.

[34]Ibid.

decided to wait until after the war ended before entertaining the idea of a separate independent Air Force. In the mean time, the Army Chief of Staff did make the U.S. Army Air Forces on par with the Ground Forces and Services of Supply.[35]

The U.S. Army Air Forces responded to the defeat at Pearl Harbor and the Philippines by expanding aircraft production, training, and research. If it were not for Arnold's intuition, dedication, and efforts towards the advancement of air power, the U.S. would have been significantly behind technologically.[36] American manufacturing plants began operating nonstop, using the innovative idea of ongoing production in conjunction with upgrading current model aircraft and developing new aircraft with the latest technology. This led to American factories producing over 324,000 aircraft during the war, roughly 134,000 more aircraft than German and Japanese factories produced combined.[37] In time, the U.S. Army Air Forces grew to 243 groups made up of 2.5 million personnel and ultimately used 35 percent of the U.S. entire budget in equipment and munitions for the war. The aviation personnel represented almost a third of the U.S. Army's overall force which further exceeded the span of control for the Army.

Unfortunately, more issues with exploiting air power continued during Operation TORCH in June of 1942. Ground commanders demanded ongoing air support for ground troops, which allowed German aviators to gain a 3-to-1 advantage in aerial victories and control of the skies. This finally led to the doctrinal change of first achieving air

[35]McFarland, 21.

[36]Daso, 94-113.

[37]McFarland, 21.

superiority before providing close air support to units on the ground.[38] It also forced air and ground commanders to coordinate efforts with each other with neither one having command over the other. This initiative proved successful in the spring of 1943 when the Allies established air superiority over North Africa, preventing the German Army in North Africa from receiving necessary supplies and reinforcements.[39]

The next major step towards an independent Air Force came in 1943 when the Army Chief of Staff, General George Marshall, issued a field manual declaring the land and air domains co-equal and co-dependent forces. The U.S. Army Air Forces began incorporating strategic bombing campaigns against critical German infrastructure.[40] The very first American strategic bombing effort already took place in April of 1942 when Lieutenant Jimmy Doolittle led a raid on Honshu, Japan with 16, B-25 Mitchell bombers but the attack caused little damage to Honshu. However, the attack did effectively embarrass Japanese military leaders, raise Allied morale, and paint an air power picture of things to come.[41] Even with the Honshu raid, strategic bombing was still relatively in its infancy and aviators gained experience through trial and error.[42]

Although the U.S. Army Air Force eventually advanced further into German occupied areas, it was at the expense of suffering significant casualties. At first, prewar

---

[38]Bernard C. Nalty, *Winged Shield, Winged Sword: A History of the United States Air Force* (Washington, DC: Air Force History and Museums Program, 1997).

[39]McFarland, 24.

[40]Ibid., 26.

[41]Ibid., 32.

[42]Ibid., 26.

doctrine determined bombers could fight and maneuver through the German air defenses unescorted After losing over 1,000 crewmembers and almost 150 bombers, a change in strategy started with long range fighters escorting bombers on missions for the duration of the war. Also, General Arnold established the U.S. Strategic Air Forces in Europe to oversee the bombing campaign against Germany. Senior aviators improved fighter tactics permitting fighters to not only escort bombers but to seek out and destroy enemy aircraft. The escorted bombers conducted a maximum offensive bombing effort targeting German aircraft manufacturing and industrial facilities. This proved too much for the German air forces leaving Germany unable to defend the skies and ultimately giving the U.S. Army Air Forces air superiority.[43]

However, using strategic bombing against key German targets ceased when General Dwight Eisenhower reallocated the air forces to focus on France, in order to again provide support to ground troops. This did provide a major advantage to the ground forces as U.S. Strategic Air Forces bombers successfully paved the way for the Third Army to go through the German lines. Additionally, fighters provided close air support for Allied soldiers moving through France to Germany. In August of 1944, air power helped in the destruction of hundreds of German armored vehicles and the capture of 50,000 German soldiers. Furthermore, the airlift and close air support provided during the Battle of the Bulge changed the tide from a near defeat to an Allied success.[44]

Despite this success, as future strategic bombing efforts confirmed, attacking the German fuel industry was more beneficial to Allied ground forces by significantly

[43]Ibid., 28.

[44]Ibid., 29.

restricting Germany's capability to fuel and mobilize their armored and mechanized units. Germany attempted to retaliate to the Allied air power by introducing the Me 262 jet fighter with intermittent success. However, Germany could not capitalize on any successes due to the impact from the strategic bombing campaign on manufacturing and industrialization facilities, leaving German aircraft and tanks powerless due to insufficient fuel. In the fall of 1944, the U.S. Strategic Air Forces in Europe began focusing strategic bombing on Germany's railway infrastructure bringing the German economy to the brink of collapse by February of 1945.[45]

Towards the end of the war against Germany, General Arnold requested a team of outside experts to conduct an objective analysis examining the successes and failures of air power. Backed by 216 volumes of analysis and records, the team produced the *United States Strategic Bombing Survey*, which determined that even Germany with a first rate military cannot overcome a force with air superiority. The report stated the initial slow production of aircraft and trained personnel, combined with misuse of bombers prevented air power from attaining its full potential. Additionally, the report highlighted the strategic bombing campaign causing Germany to focus almost half of its industry and over six million workers, soldiers, and laborers in support of aerial defense. As a result, air power helped give the Allies a significant advantage in Europe.[46]

Shifting attention to the Pacific War, the U.S. provided almost all of the forces in the theater. Unlike the war efforts in Europe, the U.S. did not have powerful allies to lean on in the Pacific. In addition, the area of operations in the Pacific was vast and contained

[45]Ibid., 32.

[46]Ibid., 33.

numerous highly fortified islands with strategic value. This enabled the U.S. Army Air Forces to play a significant part in the Pacific War.[47]

Initially, the U.S. chose to pursue a naval blockade strategy in the Pacific in order to defeat Japan. Also in the beginning, U.S. commanders did not adequately use air power in the Pacific War as the mindset was still on close air support. This proved difficult in thick jungle and rugged terrain areas like Papua New Guinea.[48] However, air power leaders focused on achieving air superiority that eventually led to the severing of Japanese resupply, reinforcement, and rescue lines in isolated areas. General Douglas MacArthur capitalized on air superiority, instituting his famous island hopping campaign using the range of aircraft capability in determining one island target to the next.[49]

The U.S. Army Air Forces also supported China in the war against the Japanese. In controlling Siam and Burma in 1942, Japan established blockades preventing China from receiving vital supplies via sea or road passages. This forced the U.S. Army Air Forces to transport supplies from India, over the extremely dangerous Himalaya Mountains using overloaded C-46 and C-47 aircrafts, into China.[50]

After three years of the U.S. pursuing the naval blockade strategy, Japan refused to surrender. However, General Arnold took advantage of the opportunity to further prove the need for an independent air force by employing a strategic bombing campaign against essential Japanese military, industrial, and economic targets. At first, the

---

[47]McFarland, 33.

[48]Ibid.

[49]Ibid., 35.

[50]Ibid.

campaign achieved very minimal success due to weather, bombing accuracy, and technical problems. However, recognizing the limited Japanese air defense systems, aircraft began flying at lower altitudes with heavier bomb loads targeting Japanese cities. As a result, in March of 1945, the U.S. Army Air Forces conducted the deadliest air assault in history by burning 15.8 square miles of urban area, killing close to 85,000 Japanese and wounding nearly 45,000, and leaving roughly one million Japanese homeless. Within five months, the U.S. Army Air Forces burned 150 square miles in 68 Japanese cities.[51]

Nevertheless, the Japanese still refused to surrender convincing President Harry Truman, facing the likelihood of a costly U.S. invasion into Japan, to authorize the first atomic bomb drop on Hiroshima, Japan on 6 August 1945 and the second atomic bomb drop on Nagasaki, Japan three days later. Strategic bombing destroyed all of Japan's major cities causing 800,000 Japanese casualties and forcing Japan to finally surrender on 14 August, 1945.[52]

Following the end of World War II, the U.S. Air Forces continued to pursue the idea of establishing a separate Air Force by creating several major commands to include; the Strategic Air Command, Air Defense Command, Air Material Command, Tactical Air Command, and the Air Transport Command. Additionally, the establishment of the civilian Scientific Advisory Group and Air University as a major command further helped the separation effort.[53]

---

[51]McFarland, 38.

[52]Ibid.

[53]Ibid., 40.

The success of strategic bombing along with the atomic bomb changed the future of warfare. The Strategic Air Command provided the world's premiere air power in delivering global long-range combat and reconnaissance operations. Additionally, the Strategic Air Command focused on the vision of helping guarantee international peace as a global nuclear deterrent. Just as the *United States Strategic Bombing Survey* stated, "the best way to win a war is to prevent it from occurring."[54]

Even though the Navy Department opposed establishing a separate air component, the War Department pushed for an independent air force with General Eisenhower leading the effort. As a result, Congress passed the National Security Act of 1947 (26 July 1947) instituting a National Military Establishment under a civilian Secretary of National Defense. This opened the door for the U.S. Air Force gaining independence on 18 September 1947.

The Ascension of Space Power

Following World War II, the Cold War conflict arose between the two super powers of the day, the democratic U.S. and the communist Soviet Union. Outer space became the new environment for the U.S. and Soviet Union to compete over for control and power. During this struggle for control over space, technology drastically improved, as did military capabilities.

The threat of a surprise nuclear attack was a primary concern of every U.S. presidential administration following World War II.[55] With the attack on Pearl Harbor

[54]Ibid.

[55]Ibid., 55.

still a close memory and the concealment of plans and operations behind the Iron Curtain, strategic reconnaissance became a main objective of space exploration. Initially, the U.S. used spy planes over the Soviet Union, beginning in July of 1956, in order to collect intelligence data and continued aerial operations until a Soviet surface-to-air missile shot down a U.S. U-2 over the Soviet Union in May of 1960.[56]

However, it was the Soviet launch of artificial earth satellites in 1957 that started the international space race. Sputnik I launched in October of 1957, gained the most attention of all the Soviet satellites. It weighed 157 pounds and remained in orbit until 1958 circling the Earth every 96 minutes. The launch of Sputnik I created mass panic across the U.S. with many citizens believing the Soviet Union had a significant advantage over the U.S. missile capabilities. This panic and belief was heightened even further when the U.S. embarrassingly failed at their first attempt to launch an American satellite in December of 1957. With television cameras recording the event, the rocket launching the satellite only lifted off the ground four feet before falling back to the ground in flames.

Public outcry forced President Eisenhower to address the incident. Eisenhower did his best to dispel the negative reactions to the failed launch and public belief that the Soviet Union had a significant advantage over the U.S. in regards to missile capabilities but he was limited in what information could be made public. Actually, intelligence gathered from U.S. spy planes showed there was a significant missile capabilities advantage but it appeared that the U.S. actually had the advantage over the Soviet Union

[56]Ibid.

in the inter-continental ballistic missiles arena.[57] However, it was the imagery collected through Project CORONA that confirmed the Soviet Union had less inter-continental ballistic missiles than the U.S.

In actuality, one satellite from Project CORONA provided intelligence analysts more images than all of the U-2 missions combined.[58] Eisenhower could not share this information with the public because it would reveal to the Soviet's that the U.S. was illegally spying over the Soviet Union. Had the Soviet's been made aware of the U.S. actions and knowledge of missile capabilities, it could have escalated hostilities between the two countries and forced the Soviet's to refocus resources towards space efforts.

Instead of going public, the President increased spending on education and international relations. In July of 1958, Eisenhower signed the National Aeronautics and Space Act paving the way for the establishment of the National Aeronautics and Space Administration (NASA) in October of 1958.[59] The intent of NASA was to enhance the level of U.S. scientific achievement and address the perceived public perception of the strategic missile capability imbalance between the U.S. and the Soviet Union. One of NASA's main priorities was exploring options for manned-space flight. The Soviet Union had already put the first living animal, a dog named Laika, in orbit around the Earth, with the launch of Sputnik II in November of 1957.

---

[57]Marta Schaff, "Sputnik & the Space Race," September 2009, http://web.ebscohost.com/ehost/detail?sid=4d701ff4-5336-4d95-8768-cf867720d04a%40sessionmgr104&vid=1&hid=128&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=khh&AN=18002119 (accessed 30 September 2013).

[58]McFarland, 56.

[59]Schaff.

NASA's budget increased nearly 500 percent from 1961 to 1964 and personnel grew to 34,000 NASA employees and 375,000 people from industry and university contractors.[60] Project Mercury and Project Gemini served the purpose of leading the way for manned-space flight. Project Mercury was NASA's first high visibility program focusing on human space flight. It focused on three primary objectives:

1. Place a manned spacecraft in orbit around the Earth.
2. Examine human performance capabilities and abilities to function in the space environment.
3. Safely recover the astronaut and spacecraft.[61]

Project Gemini exploited the successes of Project Mercury and increased the number of astronauts from one to two in a single spacecraft.[62] It also focused on three primary objectives:

1. Put humans and equipment in space flight for a period up to two weeks.
2. Rendezvous and dock with orbiting spacecrafts and maneuver the docked spacecrafts using a propulsion system.
3. Perfect procedures for reentering the atmosphere and landing at a predetermined landing point.[63]

---

[60]History.com, "The Space Race," A&E Television Networks, http://www.history.com/topics/space-race (accessed 2 October 2013).

[61]Kennedy Space Center, "Project Mercury Overview," 26 September 2000, http://www-pao.ksc.nasa.gov/history/mercury/mercury-overview.htm (accessed 30 September 2013).

[62]National Aeronautics and Space Administration (NASA), "NASA History in Brief," 20 May 2011, http://history.nasa.gov/brief.html (accessed 30 September 2013).

In addition to paving the way for NASA, Eisenhower established the National Reconnaissance Office in 1961 to lead all U.S. reconnaissance endeavors. With help from the Central Intelligence Agency and the U.S. Air Force, National Reconnaissance Office used satellite's to establish an early warning capability for the U.S. to detect a nuclear attack from opposing nations. The Air Force further developed capabilities with the Missile Defense Alarm System and later the Defense Support Program which detected missile launches almost immediately.[64]

Several more key events occurred in 1961. First, the Air Force was given responsibility for all military space operations to include the Defense Satellite Communications System I. Between 1966 and 1968, 26 satellites were launched into geosynchronous orbit in establishing the Defense Satellite Communications System I. The purpose was to provide high-volume, secure voice and data communications.[65] Second, the Defense Meteorological Satellite Program was established. The purpose of the initially classified program was to observe weather conditions around the world.[66] Third, the Space Detection and Tracking System was established for the Air Force to

---

[63]Kennedy Space Center, "Project Gemini Goals," 25 August 2000, http://science.ksc.nasa.gov/history/gemini/gemini-goals.txt (accessed 30 September 2013).

[64]McFarland, 57.

[65]Mission and Spacecraft Library, "Defense Satellite Communications System," http://space.jpl.nasa.gov/msl/Programs/dscs.html (accessed 1 October 2013).

[66]R. Cargill Hall, *A History of the Military Polar Orbiting Meteorological Satellite Program*, Office of the Historian National Reconnaissance Office, 2001, http://www.nro.gov/history/csnr/programs/docs/prog-hist-02.pdf (accessed 1 October 2013).

track and identify space debris created from space missions.[67] Fourth, the Air Force was also given the responsibility of launching all Department of Defense satellites using Cape Canaveral, Florida for launching into low inclination equatorial orbits and Vandenberg Air Force Base, California for launching into polar orbits.[68] Lastly, President Kennedy significantly expanded the U.S. Armed Forces nuclear strike capability by increasing the inter-continental ballistic missiles for the Air Force, the nuclear submarines for the Navy, and counterinsurgency capabilities for the Army. This proved especially beneficial during the 1962 Cuban Missile Crisis, when the Soviet Union retracted from Cuba based highly on the threat of the U.S. nuclear capability.[69]

Following the events of 1961, the U.S. and the Soviet Union continuously worked on a space treaty outlining acceptable operations in the space environment. After years of bargaining and debating back and forth, the Outer Space Treaty was ratified in October of 1967. In regards to arms control terms and conditions, the treaty prevents nuclear or any weapons of mass destruction from being put in orbit around the Earth or any other location in outer space to include the moon and space stations. Also, the moon and other space-based locations are to be used entirely for peaceful purposes with the establishment of military bases, weapons testing, or military exercises strictly prohibited.[70]

---

[67]McFarland, 57.

[68]Ibid.

[69]Ibid., 58.

[70]U.S. Department of State, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies," Bureau of Arms Control, Verification and Compliance, http://www.state.gov/t/isn/5181.htm (accessed 1 October 2013).

As technology continuously improved throughout the 1960s, so did space capabilities. In July of 1969, the U.S. accomplished one of the greatest technological achievements in history when Neil Armstrong became the first human to walk on the surface of the moon.[71] This achievement officially ended the space race and cemented the U.S. on the top of the space frontier over the Soviet Union. Three years later, Dr. Werner von Braun envisioned, "One hundred years from now, people will look back and wonder how man could ever have managed his affairs on this planet without the tools provided by the space program. That there ever could have been a world without spacecraft will be just as difficult for them to perceive as for us to imagine living in a world without telephones or airliners."[72]

Although the moon landing ended the space race, the potential threat of attacks from space still existed. Even with the Anti-Ballistic Missile Treaty signing by the U.S. and Soviet Union in 1972, the U.S. was still concerned with its defense capabilities to effectively thwart any nuclear strikes from the Soviet Union. President Nixon initiated and President Carter expanded a counterforce targeting capability during the 1970s but President Reagan instituted the Strategic Defense Initiative in the 1980s. One of the Strategic Defense Initiatives focused on developing space-based lasers to intercept incoming Soviet inter-continental ballistic missiles. As a result, the Alpha HF space-

[71]Jennifer Rosenberg, "First Man on the Moon," About.com Education 20th Century History, http://history1900s.about.com/od/1960s/p/firstmanmoon.htm (accessed 30 September 2013).

[72]Michael C. Whittington, *A Separate Space Force, An 80-Year-Old Argument,* Maxwell Paper No. 20 (Maxwell AFB, AL: Air War College, May 2000), 1.

based laser was developed and proved that successfully building and operating space-compatible lasers is possible.[73]

By the time Operation Desert Storm occurred in 1991, the U.S. military was heavily dependent on space. Using space assets, over 1,200 combat sorties were executed and 106 cruise missiles launched within the first 14 hours of the conflict. This was the first high profile demonstration on the capabilities and benefits of space forces.

Today, the military is even more dependent on space capabilities that provide missile warning and defense, global communications, navigation, intelligence, surveillance, and reconnaissance. The civilian sector also depends on space and has become a part of everyday life. Television is broadcast all over the world via satellite. Satellites help forecast our weather, days to weeks ahead of time. Global positioning systems are almost standard in most cars. The aviation community extensively uses space-based capabilities. The global space revenue from government and private sources has reached over $289 billion annually.[74]

The Emergence of Cyber Power

One of the first major cyber attacks in history occurred in 1982 when Soviet spies stole a computer-control system from a Canadian firm. Unbeknownst to the Soviets, the Central Intelligence Agency configured the system software to overload pipeline joints

[73]Melissa Olson, "History of Laser Weapon Research" (Naval Surface Warfare Center, Dahlgren Division, Corporate Communication, 2012), www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA557756 (accessed 1 October 2013), 32.

[74]Space Foundation, "2012 Annual Report," http://www.spacefoundation.org/docs/SF-2012-annual-report.pdf (accessed 2 October 2013).

and welds with excessive pressures that ignited the largest non-nuclear explosion ever seen from space.[75]

Although this cyber attack occurred over three decades ago, the cyber threat has just come to the forefront and focus of the U.S Government within the last decade. In the 1982 cyber attack, there were multiple entities involved with cyber only really being used in the delivery outcome of the mission. There was still a significant physical real world entity required for the operation, in that the Soviets had to physically steal the malicious software and then physically upload it into their system.

Today, most systems are connected to a network which can be accessed remotely from unauthorized users, meaning cyber attacks are no longer as dependent on the real world physicality. Prior to the last decade most cyber attacks were usually only seen in science fiction movies and—or read in science fiction novels. So what changed? The fact that we are now more globally connected and dependent upon cyber greatly increases the threat to our national security.

The U.S. intelligence community releases the Worldwide Threat Assessment every year that provides an assessment of global threats. Since 9/11, terrorism has ranked as the number one security threat facing the U.S. However, the most recent threat assessment released in March 2013 now identifies cyber attacks and cyber espionage as the new top security threat. Cyber is intertwined with our vital infrastructures, economy,

[75]Matt Murphy, "Cyberware: War in the Fifth Domain," *The Economist*, 1 July 2010, http://www.economist.com/node/16478792 (accessed 30 March 3013).

and personal lives and digital technologies are employed globally faster than our ability to comprehend the effects on security against potential threats.[76]

Many current state and nonstate actors use cyber to accomplish strategic goals with achieving cyber superiority as a top priority. Using cyber capabilities to achieve strategic objectives are increasing at a substantial rate. However, the policy and regulations for using these capabilities cannot keep the same pace, potentially leading to unintended consequences.[77]

Just like a significant kinetic attack on U.S. soil from opposing nations is unlikely in the near future, so is a significant cyber attack. However, as technological advances continue and criminals, opposing nations, and terrorists become more cyber sophisticated, the threat of a significant cyber attack against essential U.S. infrastructure resulting in long-term and wide-scale disruption exists. In the mean time, more likely threats in the next couple of years come in the form of highly motivated aggressors seeking a back door to vulnerable nodes that manage critical systems (i.e. power grids), but the current advantages of any unauthorized access are believed to be limited and short term. Additionally, even greater threats are from unforeseen system designs and errors that corrupt one system and then infect other systems across the network.[78]

---

[76]James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community* (Director of National Intelligence, 12 March 2013), http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf (accessed 30 March 2013), 1.

[77]Ibid.

[78]Ibid.

Over the last several years, foreign intelligence agencies have consistently hacked into unclassified U.S. Government cyber networks. This exposes a major weakness in our data security considering most of the countries and our allies' proprietary data are stored on unclassified networks. Adversaries are stealing technology and trade secrets that traditionally afforded the U.S. distinct worldwide military advantages.

Even more discouraging, foreign cyber adversaries are also targeting and seeking unauthorized access to classified networks as well. Potentially, they may obtain access to critical information such as plans and intentions, current and future operations, advanced capabilities, secure email traffic, secure websites and databases, and classified reports. Again, this not only allows U.S. adversaries to level the military playing field but also allows the adversaries to manipulate the data gathered providing the same advantages the U.S. previously enjoyed.

For example, it was reported in May of this year that Chinese military hackers stole blueprints and data pertaining to two dozen weapons systems that are critical to U.S. national security, to include the F-35 Joint Strike fighter, F/A 18 fighter jet, V-22 Osprey, PATRIOT Missile, Littoral Combat Ship, Blackhawk Chopper, the Navy's ballistic missile interceptor technology, Aegis and the Army's ballistic missile interceptor program, and Terminal High Altitude Area Defense. Although some experts argue that the Chinese will still not be able to produce a stealth fighter with the stolen information, however, the Chinese will be able to identify U.S. stealth capabilities and potential

weaknesses in design. Through these cyber hacks, the Chinese military saved billions of dollars and 25 years of research and development.[79]

A significant concern for the U.S. and other global cyber players is online information control. However, there are fundamental differences on the definition of cyber threats between the U.S. and other nations (i.e. Russia, China, and Iran). The U.S. concentrates on cyber security and the threats to the accuracy and authenticity of its networks and systems.[80]

Communication systems, air traffic control systems, orbiting satellites, oil refineries, pipelines, transportation systems, financial institutions, and power grids are all cyber dependent and vulnerable to attack. Any focused attack on just one of these critical nodes can cause significant infrastructure and economical devastation along with potential loss of life. A sophisticated attack on multiple nodes can lead to a catastrophic economic meltdown causing widespread panic and death.

A comparable incident is immediately following 9/11 when the stock market was intentionally closed for four trading days. This led to the Dow declining 7.3 percent the day it reopened, creating the worst single day loss in history and extended the recession.[81] In addition, after experiencing profitability the six consecutive years prior to 9/11, the

---

[79]Jack Mick, "Chinese Hackers Score F-35, Black Hawk Chopper, and PATRIOT Missile Data," *Daily Tech*, 28 May 2013, http://www.dailytech.com/Chinese+Hackers+Score+F35+Black+Hawk+Chopper+and+PATRIOT+Missile+Data/article31638.htm (accessed 1 November 2013).

[80]Clapper, 2.

[81]Kimberly Amadeo, "How the 9/11 Attacks Still Affect the Economy Today," US Economy.About.com, 2013, http://useconomy.about.com/od/Financial-Crisis/f/911-Attacks-Economic-Impact.htm (accessed 30 March 2013).

airline industry saw a net loss of $74 billion from 2001 to 2010.[82] This does not include the estimated $600 billion in revenue lost by hotels, restaurants, retailers, etc. from declined tourism in major cities around the U.S.[83]

In March 2013, the head of U.S. Cyber Command, General Keith Alexander, testified on Capitol Hill that cyber attacks on our critical systems would cause as much or greater damage than occurred from 9/11.[84] In September 2012, major banks such as Bank of America, JP Morgan Chase, Wells Fargo, U.S. Bank, and PNC Bank were hit with their biggest cyber attack in history.[85] Even though the attacks were denial of service attacks that made their respective websites inaccessible, it still demonstrates how susceptible online systems are to cyber attacks.

A more recent incident occurred on 23 April 2013 with the Syrian Electronic Army hacking into an Associated Press twitter account and posting a false tweet stating that two explosions occurred in the White House and President Barack Obama was injured. This hack caused the Dow Jones industrial average to drop more than 128 points

---

[82]Bill Poling, "10 Years: How 9/11 Changed Travel?" *Travel Weekly*, 31 August 2011, http://www.travelweekly.com/travel-news/travel-agent-issues/10-years--how-9/11-changed-travel/ (accessed 30 March 2013).

[83]Georgette Jasen, "Economic Cost of 9/11: Three Industries Still Recovering," *The Fiscal Times*, 9 September 2011, http://www.thefiscaltimes.com/Articles/2011/09/09/Economic-Cost-of%209-11-Three-Industries-Still-Recovering.aspx#page1 (accessed 30 March 2013).

[84]Tom Gjelten, "Is All The Talk About Cyberwarfare Just Hype?" National Public Radio, 15 March 2013, http://www.npr.org/2013/03/15/174352914/is-all-the-talk-about-cyberwarfare-just-hype (accessed 30 March 2013).

[85]David Goldman, "Major Banks Hit with Biggest Cyber Attack in History," *CNN Money*, 28 September 2012, http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html (accessed 30 March 2013).

immediately following the tweet.[86] Cyber attacks currently account for tens of billions of dollars in U.S. economic loss annually.[87]

In regards to threats to U.S. military operations, about 90 percent of military cyber networks utilize commercial infrastructure.[88] A 2012 study from Security and Defense Agenda reported that 57 percent of global experts surveyed believe an arms race in cyberspace is already in progress.[89] The three major U.S. cyber threats come from terrorist organizations, hacktivists, and cyber criminals.

Terrorist organizations are increasing their offensive capabilities. Hacktivists traditionally pursue businesses and organizations using denial of service attacks that prevent users from accessing networks or they leak personal information (i.e. credit cards, social security numbers, phone numbers, etc.). Cyber criminals present the most dangerous threat to U.S. economic interests. They are highly competent and sell cyber intrusion equipment to the highest bidder. This provides access to key infrastructure systems allowing criminals, state actors, and non-state actors to steal, manipulate, or

---

[86]David Jackson, "AP Twitter Feed Hacked; No Attack At White House," *USA Today*, 23 April 2013, http://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/?morestories=obnetwork (accessed 24 April 2013).

[87]Marck Hosenball and Patricia Zengerle, "Cyber Attacks are Leading Threat Against U.S.: Spy Agencies," *NBC News.com*, March 2013, http://www.nbcnews.com/technology/technolog/cyber-attacks-are-leading-threat-against-us-spy-agencies-1C8830308 (accessed 30 March 2013).

[88]Rob McIlvain, "Army Sees Cyber Threats as Imminent," The Official Homepage of the United States Army, 28 October 2011, http://www.army.mil/article/68283/ (accessed 30 March 2013).

[89]Suzanne Kelly, "Government not keeping Pace with Cyber Threats," *CNN.com*, 1 February 2012, http://security.blogs.cnn.com/2012/02/01/government-not-keeping-pace-with-cyber-threats/ (accessed 30 March 2013).

delete critical information.[90] As mentioned previously, foreign governments are already using intrusion equipment to infiltrate U.S. networks.

[90]Clapper, 3.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter contains the methods used to answer the primary as well as the secondary research questions. This study uses a qualitative analysis and comparison of current cyber threats, capabilities, policy, strategy and organization to determine similarities between events experienced during the emergence of air and space power.

The research is organized into three parts overall. First, U.S. air power is examined to understand the history and environment leading up to the establishment of the U.S. Air Force. Second, U.S. space power is researched to appreciate the background of how the military and civilian sector became space dependent. Third, an overview of cyber is provided to include current worldwide cyber threats and capabilities.

The results of these three components are then analyzed. Based on the analysis, for the evaluation study portion of this thesis, I examined the different options for the Department of Defense to organize cyber operations. I investigated the best options to proceed with cyber operations into the future, based on the results of the findings and analysis study portion of the thesis. I used books, articles, papers, congressional hearings, speeches, and military publications to conduct my research.

CHAPTER 4

FINDINGS AND ANALYSIS

Like the Army using hot air balloons in the air domain and the Air Force using satellites in the space domain, cyber military operations initially focused on intelligence, surveillance, and reconnaissance. However, when cyber capabilities are recognized as a weaponized system for offensive and defensive operations, the potential resembles a more traditional military combat power (i.e. fighter jets, tanks, missile silos, and other offensive and defensive weapons) within the U.S. arsenal.

Limited air capability and technology during World War I and the interwar periods negated the significance that air power played in modern warfare. However, as technological advances in aviation increased, so did the capabilities and threats from the air. Still, senior military and government leadership for several years failed to recognize the strategic impact aviation made in the battlefield. The air campaign results during World War II and the advent of the global nuclear threat capability cemented the Air Force's place in history.

The space race made the space domain relevant but treaties and economics prevented the need for a separate space service. Without the peace treaties established decades ago, it is very likely that the focus on developing offensive capabilities in space would have continued providing an entirely different threat that we are accustomed to today. Also, the amount of money it costs to put assets and equipment into space allows most nations to focus on other endeavors.

So where does cyber fit into the air and space history. Just like the competition for air and then space dominance during the 20th century, the race for cyber control and

dominance is happening now. Similar to air and space opponents during their respective rise to power, threats in cyber today are also downplayed as insignificant by many leaders. Also, a parallel exists between cyber and the rise of air and space, in that as technological advances occur, so do the capabilities and threats to the U.S.

The following provides those threats and capabilities, what the U.S. Government is doing to combat and take advantage of threats and capabilities, and also draws comparisons to the rise of air and space power.

Only Cyberwarriors can Understand Cyber Power

Similar to the senior military beliefs and understanding during the emergence of air power, many senior military leaders today still only recognize cyber for its non-kinetic capabilities and for its support roles to other domains. A kinetic cyber attack could be a hacker gaining access to the control system of a dam and then opening the dam to flood a town or city. At its core, with the world wide dependence on cyber and threats therein, it is a strategic weapon. Even former National Security Agency Director, Mike McConnell, equates cyber attacks to weapons of mass destruction.[91]

Unofficially, the reported U.S. and Israel Stuxnet cyber attack that destroyed centrifuges at an Iran nuclear facility in 2010 is a prime example of kinetic cyber capabilities. The Stuxnet computer virus claims to have ruined the electric motors of the centrifuges by accelerating the motors to destructive speeds. As a result, the Iranian

[91]Anna Mulrine, "Cyber Security: The New Arms Race for a New Front Line," *The Christian Science Monitor*, 15 September 2013, http://www.csmonitor.com/USA/Military/2013/0915/Cyber-security-The-new-arms-race-for-a-new-front-line (accessed 3 October 2013).

nuclear program was supposedly delayed by two years.[92] Although the U.S. and Israel have neither confirmed nor denied their involvement, the fact is there was a cyber attack against Iran's nuclear program.

Officially, the Air Force has already proven in cyber simulations the capability to take control of enemy rocket launchers and launching either away from friendly forces and assets or targeting enemy assets with their own rocket.[93] The idea of independent operations is difficult to grasp for senior leaders. This appears eerily familiar to the U.S. Army's pre-U.S. Air Force belief and understanding of air power. As previously reported, this caused significant conflicts between air and ground leaders during the interwar and World War II periods on how air power should be executed.

The threat of being attacked from the skies above via conventional and non-conventional weapons, puts air power in the forefront of military importance since the early part of the 20th century. The significance of air superiority has proven even clearer during the first Gulf War and the more recent conflicts in Iraq and Afghanistan. U.S. ground forces were never concerned about attacks from enemy aircraft above, whereas U.S. air power significantly limited enemy operations and movement. The average response time for close air support was around 12 minutes from the time it was requested by ground commanders but this was only possible in a mature theater in which the U.S. controlled the entire air space.

---

[92]George Putic, "Stuxnet: An Effective Cyberwar Weapon," Voice of America, 28 June 2013, http://www.voanews.com/content/stuxnet-an-effective-cyberwar-weapon/1691311.html (accessed 3 October 2013).

[93]Mulrine.

The major strategic threats in the cyber domain are similar now to what air and space power experienced. For example, the potential is there to hack and exploit U.S. power grids, derail trains, shutdown financial networks, disable weapons systems, and contaminate water supplies. The threat of a "Cyber Pearl Harbor" is one of the Department of Defense's biggest fears. However, one major difference between the air and space domains with the cyber domain is the non-strategic threats to civilians. For example, personal computers, bank accounts, email accounts, credit card numbers, home security systems, televisions, and web-cameras are all vulnerable to cyber attacks. Additionally, a growing number of new vehicles manufactured are vulnerable to hackers taking control of the cars brake system, power steering, global positioning system, speedometers, and cruise control via the vehicles wireless and Bluetooth connections.[94]

This expands the "cyber battlefield" worldwide and to everyone using any device or system with network connection capabilities. Furthermore, there is a cyber race similar to the space race during the Cold War but the U.S. is competing with many more entities than just the Soviet Union this time. Nations states, terrorist organizations, individual hackers, ignorant cyber enthusiasts, and insider threats are all players in the cyber race and equally dangerous.

[94]Andy Greenberg, "Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel," *Forbes*, 24 July 2013, http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/ (accessed 3 October 2013).

Cyber Leadership Demands Operational Experience

In October 2010, U.S. Cyber Command became fully operational as a sub unified command under U.S. Strategic Command. U.S. Cyber Command's mission is to plan, coordinate, integrate, synchronize, and conduct activities to:

1. Direct the operations and defense of the Department of Defense Information Networks,
2. Strengthen the U.S. ability to resist and respond to cyber attacks,
3. Conduct a full range of military cyberspace operations in order to enable capabilities in all domains,
4. Provide support to combatant commanders for conducting their missions globally,
5. Ensure U.S. and its allies autonomy in cyberspace to freely conduct operations and deny our adversaries from achieving the same opportunity.[95]

The Command is in the process of establishing a cyber force structure in addition to developing training requirements and certification standards for all the military service elements (i.e. Army Cyber Command, Air Forces Cyber, Fleet Cyber Command, and Marine Forces Cyber Command) to use in building their respective cyber force.[96]

Within the last few years, service components have just started training the next generation cyber experts. This poses potential gaps in U.S. offensive and defensive capabilities, in that U.S. global adversaries are improving in the cyber arena much faster

[95]U.S. Strategic Command, "U.S. Cyber Command," Fact Sheets, August 2013, http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 3 October 2013).

[96]Ibid.

and better than the U.S initiatives. One such initiative that is gaining notoriety is the establishment of cyber ranges, such as CyberCity.

CyberCity, an 8-by-10 model town, was developed in response to the U.S. Air Force's need to improve cyberwarriors offensive and defensive cyber skills. This simulated city contains model trains, miniature cellphone towers, and streetlights which are all connected to a miniature power grid.[97] The concept is similar to a flight simulator and supports 30 to 50 trainees at a time. The simulations require trainees to hack into physical cameras that are located all through the model city in order to gain access to the streaming video feed. Then, the trainees are given various missions to execute (i.e. prevent terrorist attacks on a reservoir, derailing a train carrying nuclear materials, hacking into the power grid, and preventing attacks). Trainees also gain knowledge on taking control of external computers and employing reverse engineering (i.e. take control of enemy rocket launchers and using digital forensics to collect intelligence left behind by adversaries). The realistic simulations prepare trainees to understand back-end systems that manage real world critical systems.[98]

The Fifth Dimension of Warfare

The creation of boats and ships yielded navies and the development of the airplane gave rise to air forces. The stage is being set for the ascension of cyber forces. U.S. Cyber Command is increasing its cyber personnel from 900 to 4,900 over the next

[97]Mulrine.

[98]Nicole Johnson, "CyberCity prepares Air Force for Cybersecurity," *Federal Times*, 11 December 2012, http://www.federaltimes.com/article/20121211/IT01/312110004/CyberCity-prepares-Air-Force-cybersecurity (accessed 3 October 2013).

two years. The personnel will be divided among three forces; the national mission forces, cyber protection forces, and combat mission forces. The national mission forces will have specialized training in protecting critical infrastructure (i.e. power grids and water supplies). The cyber protection forces will defend the Department of Defense Information Networks. The combat mission forces are in charge of counterattacks and additional offensive operations.

The 900 to 4,900 increase in personnel is significant but is it enough to meet the growing demands and threats faced in cyberspace. According to the commander of Air Forces Cyber, Major General Suzanne Vautrinot, she believes there is a necessity for 20,000 to 30,000 cyberwarriors with the highest level of expertise and further stated, "Cyber is foundational to everything we do, because everything you do in your mission is dependent on it."[99]

Early air and space proponents spent years convincing the government and military leaders of the day that vital national assets were no longer protected by their armies from air and space attacks. The air attacks on Pear Harbor were severe enough for the U.S. to officially enter World War II. The threat of nuclear launches on earth-bound targets prompted a space treaty. A similar threat now exists in the cyber domain but we no longer have the luxury of focusing on a handful of adversaries as cyber attacks can come from anyone, anywhere, and at anytime across the globe without warning.

Furthermore, depending on the sophistication of the attack, targets may not know who conducted the attack or even recognize they were attacked at all. Additionally, the capability exists to conduct attacks on targets but disguise the culprit as someone else.

[99]Mulrine.

The Stuxnet attack on Iran may have come from a different nation other than the U.S. and Israel or Iran could have unintentionally caused the damage themselves but saw an opportunity to hold others responsible. This presents challenges that are unseen in the other domains, as there are existing advantages the U.S. has in the air and space domain not afforded in the cyber domain. For example, the U.S. has the world-wide capability to monitor air traffic and detect, within seconds, any inter-continental ballistic missiles launched.

All of the ships, planes, and ground forces in the world cannot thwart the millions of daily cyber attacks against the U.S. Government, civilian organizations, and civilian populace. Very few nations, if any, can compete with the U.S. firepower and combat capability provided by the military service components. Our adversaries will attack the U.S. at its weakest point, which is arguably in the cyber domain. The cyber medium is not limited to ground, sea, air, and space as wireless technology encircles almost every populated area across the world making the medium difficult to avoid.

Service Survival of the Fittest

With drawdown of operations in Iraq and Afghanistan, all the military services are expected to reduce their forces. Over the next five years, the Army is scheduled to downsize from 570,000 to 490,000 troops, the Marine Corps is scheduled to downsize from 202,000 to 182,000 troops.[100] The Air Force and Navy are expected cuts as well but not to the degree of the Army and Marine Corps. As cyber is the current medium gaining

[100]Thom Shanker, "Hagel Gives Dire Assessment of Choices He Expects Cuts to Force on the Pentagon," *New York Times*, 31 July 2013, http://www.nytimes.com/2013/08/01/us/politics/hagel-sees-2-paths-for-cuts-paring-militarys-size-or-capability.html (accessed 4 October 2013).

most of the attention, each service wants as much of the cyber responsibility as possible. With any increased responsibility, typically comes more manpower and more funds.

However, senior military leaders must be careful that manpower and money are used for cyber programs and not other self servicing initiatives. For example, if a military service is given a specific cyber responsibility and funding to go with it, what is the assurance the funding will go towards cyber. Per the commander of Air Force Space Command, General William Shelton, one of the top current space initiatives is the "Space Fence", which is intended to track space debris to prevent countless pieces of orbiting rock, trash, etc. from colliding with satellites causing billions of dollars in damage.[101] However, funding is in jeopardy due to Department of Defense budget cuts. The question is how does the Space Fence initiative rack and stack against other Air Force priorities. Could space be losing a significant necessity based on being under the big Air Force umbrella?

Government and Civilian Disconnect

Unlike experiences in the air and space domains, lack of public support for the government protecting and operating in the cyber domain is becoming more of an issue. Although the threats in cyberspace are apparent and must be addressed, there are also concerns from the public on how protection is accomplished. A growing number of the American public want to be safe and secure in the cyber domain but not at the risk of losing their privacy.

---

[101]David M. Ewalt, "Budget Cuts Threaten the Air Force's New Space Fence," *Forbes*, 17 July 2013, http://www.forbes.com/sites/davidewalt/2013/07/17/budget-cuts-threaten-the-air-forces-new-space-fence/ (accessed 4 October 2013).

The recent events of a former government contractor, Edward Snowden, leaking National Security Agency surveillance, heightened the privacy concern debate in the public.[102] Also, private organizations are leery about giving the government access to their network systems for fear of giving away trade secrets to the government. Instead, these organizations are investigating the legality of conducting their own counterattacks to retrieve stolen information resembling the Wild Wild West environment. Advocates believe organizations have the right to protect information without going to the authorities first. Others believe that it is unrealistic to expect organizations to defend cyber attacks from foreign nations. This makes the way ahead for military cyber operations even more complex as the commander of U.S. Cyber Command, General Alexander, stated that, "I think this gets to the heart of how do we defend the country, and when does the Defense Department step in to defend the country?"[103]

This study identified the positive and negative lessons learned during the emergence of air and space power, to determine applicability to today's challenges with the emergence of cyber power. To accomplish this objective, this chapter highlighted the lessons learned from air and space and how those lessons are relevant today. Specifically, this chapter presented why we need cyber professionals at the senior leadership level, especially in senior level cyber positions. Furthermore, we must properly groom these next generation cyber leaders through adequate cyber operational experience. The number of cyber professionals needed to adequately operate in the cyber domain will increase significantly over the next few years. Oversight is needed to ensure cyber

[102]Mulrine.

[103]Ibid.

funding goes to cyber initiatives and not rerouted to support service specific requirements. Finally, this chapter determined why policies and laws must be developed to determine not only how the U.S. Government operates in cyber, but also the private sector.

This chapter presented various challenges the U.S. Government is currently facing in the cyber domain and how we faced these similar challenges during the emergence of air and space power. Left unchecked, these challenges can potentially jeopardize U.S. national interests as presented earlier in this study. In order to mitigate these challenges, the following chapter provides recommendations to consider for implementation or to conduct further research.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

The U.S. and its allies will continue to face an ever growing cyber threat. This thesis focused on identifying positive and negative lessons learned during the emergence of air and space power, to determine applicability to today's challenges with the emergence of cyber power. This study highlighted the challenges the air and space community faced initially and how they overcame the challenges. Additionally, the current U.S. cyber posture along with potential threats and vulnerabilities to the military and civilian sector were examined. The objectives in this study were obtained through examining the emergence of air and space power and comparing it to current U.S. cyber, policies, strategies, and regulations. In describing the current U.S. cyber posture, this study highlighted the similarities between cyber and the initial air and space policy and organization.

Only Cyberwarriors can Understand Cyber Power

Just like the air, sea, ground, and space domains, cyber needs senior leaders who are competent, experienced, and prepared in understanding the threats, capabilities, and potential in the cyber domain. It needs leaders who not only advocate for the capabilities provided to the individual soldier, airman, seaman, and marine but also at the strategic level in providing capabilities to the entire military as a whole. These leaders should not only be put in position in the cyber environment but also at the strategic level all the way to the top of the military chain of command. Only then, will cyber have a true advocate that can speak to the way ahead for the domain.

Cyber Leadership Demands Operational Experience

It will take time to grow and groom the next generation of cyber leaders. With advanced cyber schools and training only being established in the last few years, a gap in operational experience exists within the cyber domain. Cyber criminals and hactivists are years ahead of the military from a cyber operational mindset. Additionally, it is important to distinguish that cyber is no longer merely a support function to the warfighter but is now a critical and active component as a warfighting function.

The U.S. military must recognize that it will take time and a significant amount of money to adequately train cyber professionals. Therefore, the military must ensure it capitalizes on their investment. Similar to Air Force aviators accruing a 10 year commitment following pilot training, cyber professionals should be required to serve between six and ten years depending on the track taken (i.e. offense or defense) and the level of training provided. The actual costs of adequately training cyber professionals should be further examined to determine the cost benefit to the military member and the U.S. Government.

The Fifth Dimension of Warfare

Notwithstanding the Department of Defense's efforts to address current and future cyber threats, the U.S. Government is still not meeting the needs required to effectively operate in the cyber domain. Considering the rapid growth in technology, the lack of operational experience, the time required to adequately train cyberwarriors, and the dependence on cyber in the government, public, and private communities, defending the U.S. and exploiting the offensive capabilities in cyber is a complex dilemma. Because of

rapidly evolving technology, and the cost of implementing changes across expansive government architecture, cybersecurity is a complex and difficult problem. As a result, the U.S. remains highly vulnerable to cyber attacks of epic proportions. The following are four options to consider for implementation or for conducting additional research in regards to moving forward in the fifth dimension of warfare:

Option 1: Establish U.S. Cyber Command as a Combatant Command: Offensive and defensive operations in cyberspace go beyond the traditional domains of conflict. Since cyberspace is completely different from the land, sea, air, and space domains, it justifies the necessity to elevate from a sub unified command of the U.S. Strategic Command to an independent Combatant Command. This is especially true considering the number of additional cyber experts currently needed is at least 20,000 to 30,000 personnel.

Option 2: Integrate U.S. Cyber Command to the U.S. Special Operations Command: One of the advantages and disadvantages of cyber is the capability to attack without a target knowing who did it or even recognizing the attack in the first place. As the U.S. military becomes more proficient, the power to conduct intelligence, surveillance, and reconnaissance and offensive attacks covertly in the cyber domain provides a vital capability to the U.S. arsenal. For example, the ability to deter the manufacturing of nuclear weapons (i.e. Stuxnet to Iran), meets the strategy of protecting U.S. national interests. Also, other black operations may become necessary without it being scrutinized in the public forum (i.e. influencing governments or providing support to specific leaders around the world). Again, this may prove more difficult or illegal if and when international cyber laws are agreed upon.

Option 3: Establish the U.S. Cyber Force as a an Independent Military Service: Since cyber is currently the domain garnering the most attention and concern, it may warrant having its own separate military service. The land, air, and sea already have their own services so there is a valuable argument. Those opposing argue that there is not a separate military service for the space domain or a need for one. However, there is a significant difference between operations in cyber from the space domain. First, the Space Treaty regulates what type of operations can be conducted in space making current threats minimal. Second, it is extremely expensive to operate in space limiting the number of nations who can support operations. Currently, less than 30 countries across the globe have assets in space. Third, the U.S. can identify space launches within in seconds of lift off, making it very difficult for adversaries to conduct any type of covert operations.

In contrast to the cyber domain, there are no binding international agreements or treaties regulating operations in cyberspace leaving it to each individual country to decide what is legal or not. The low cost of cyber capabilities opens up the threat of cyber attack not only to nation states, but terrorist organizations and other entities wishing to do harm to the U.S. Insider threat within cyber is equally dangerous at levels unseen in the other domains. Lastly, identifying cyber attacks and the culprit behind the attacks can be extremely difficult to ascertain. Unfortunately, it may take a momentous cyber attack on crucial U.S. infrastructure before it is realized if there truly is a need for cyber independence.

Option 4: Maintain Current Progress: The Department of Defense has made significant strides in cyber development in a short period of time. Establishing the U.S.

Cyber Command and respective cyber service commands demonstrates senior government and military leaders comprehend the importance of operating in the cyber domain and the impact on national interests. It is possible that an effective world-wide cyber treaty can be signed that mitigates many of the existing cyber threats. Furthermore, a catastrophic cyber attack against U.S. power grids, financial systems, water supplies, and other vital infrastructure may never occur. It is possible that the U.S. is able to adequately secure vulnerable systems or effectively defend against incoming cyber attacks. Also, the U.S. Government and private sectors may work out an agreement with the government playing only a minor role in securing and defending non-government systems. With these changes in the cyber community, the importance and impact of cyber in military operations lessens considerably.

Service Survival of the Fittest

The growth of the cyber domain is imminent and the U.S. Government must make certain that cyber priorities are established and executed without interference from other services priorities. As each service attempts to take their respective piece of the "cyber pie," the military must carefully scrutinize not what is in the best interest of the service components but what is in the best interest of cyber. Learning from past experience during the emergence of air and space power, the same lessons hold true today. In a sense, the service components should be asking not what cyber can do for them but what they can do for cyber.

Government and Civilian Disconnect

The U.S. should be extremely careful in allowing companies to retaliate against cyber attacks on their respective networks. Corporations could retaliate against the wrong organization or exceed the intended level of counterattack warranted, which could result in escalating a situation that threatens U.S. national security.

The U.S. Government and private industry must collaborate on a solution that provides the necessary defense of the U.S. networks, infrastructure, and economy. International laws and policies need to be established that outline what is and what is not acceptable in the cyber domain. Consequences for failing to meet the agreements must also be identified and strictly enforced. Additionally, an agency or department should be identified to oversee and enforce the laws. Proper procedures must be established for private organizations to report cyber attacks on their network without compromising trade secrets.

Summary

The current operating environment in cyber is challenging and complex. Capabilities, threats, and vulnerabilities in cyber are changing daily. It is important for the U.S. Government to get ahead of these challenges and provide an adequate defense to vital U.S. infrastructure and in turn capitalize on the offensive opportunities presented to our military forces. Each recommendation provided in this chapter provides a different way ahead for cyber operations but no recommendation is perfect or complete. I offer each recommendation to be studied more extensively in order to determine the validity and feasibility or if other recommendations make sense given the ever changing cyber environment.

BIBLIOGRAPHY

Amadeo, Kimberly. "How the 9/11 Attacks Still Affect the Economy Today." US Economy.About.com, 2013. http://useconomy.about.com/od/Financial-Crisis/f/911-Attacks-Economic-Impact.htm (accessed 30 March 2013).

Clapper, James R. *Worldwide Threat Assessment of the US Intelligence Community.* Director of National Intelligence, 12 March 2013. http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf (accessed 30 March 2013).

Daso, Dik. "Origins of Airpower." *Airpower Journal* 11, no. 3 (Fall 1997): 94-113. http://search.proquest.com/docview/217772366?accountid=28992 (accessed 1 November 2013).

Ewalt, David M. "Budget Cuts Threaten the Air Force's New Space Fence." *Forbes*, 17 July 2013. http://www.forbes.com/sites/davidewalt/2013/07/17/budget-cuts-threaten-the-air-forces-new-space-fence/ (accessed 4 October 2013).

Gjelten, Tom. "Is All The Talk About Cyberwarfare Just Hype?" National Public Radio, 15 March 2013. http://www.npr.org/2013/03/15/174352914/is-all-the-talk-about-cyberwarfare-just-hype (accessed 30 March 2013).

Goldberg, Alfred. *A History of the United States Air Force 1907-1957*. Princeton: D. Van Nostrand Company, 1957.

Goldman, David. "Major Banks Hit with Biggest Cyber Attack in History." *CNN Money*, 28 September 2012. http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html (accessed 30 March 2013).

Greenberg, Andy. "Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel." *Forbes*, 24 July 2013. http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/ (accessed 3 October 2013).

Hall, R. Cargill. *A History of the Military Polar Orbiting Meteorological Satellite Program.* Office of the Historian National Reconnaissance Office, 2001. http://www.nro.gov/history/csnr/programs/docs/prog-hist-02.pdf (accessed 1 October 2013).

Harter, Mark E. "Ten Propositions Regarding Space Power: The Dawn of a Space Force." *Air & Space Power Journal* 20, no. 2 (2006): 64-78, 126. http://search.proquest.com/docview/217768160?accountid=28992 (accessed 3 October 2013).

Hearn, Chester. *Air Force: An Illustrated History*. Minneapolis: Zenith Press, 2008.

History.com. “The Space Race.” A&E Television Networks. http://www.history.com/topics/space-race (accessed 2 October 2013).

Hosenball, Marck, and Patricia Zengerle. “Cyber Attacks are Leading Threat Against U.S.: Spy Agencies.” *NBC News.com*, March 2013. http://www.nbcnews.com/technology/technolog/cyber-attacks-are-leading-threat-against-us-spy-agencies-1C8830308 (accessed 30 March 2013).

Jackson, David. “AP Twitter Feed Hacked; No Attack At White House.” *USA Today*, 23 April 2013. http://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/?morestories=obnetwork (accessed 24 April 2013).

Jasen, Georgette. “Economic Cost of 9/11: Three Industries Still Recovering.” *The Fiscal Times*, 9 September 2011. http://www.thefiscaltimes.com/Articles/2011/09/09/Economic-Cost-of%209-11-Three-Industries-Still-Recovering.aspx#page1 (accessed 30 March 2013).

Johnson, Nicole. “CyberCity Prepares Air Force for Cybersecurity.” *Federal Times*, 11 December 2012. http://www.federaltimes.com/article/20121211/IT01/312110004/CyberCity-prepares-Air-Force-cybersecurity (accessed 3 October 2013).

Joint Education and Doctrine. “Joint Publication 3-12, Cyberspace Operations-Unclassified Excerpts.” *Joint Doctrine Update* 8, no. 2 (April 2013).

Joint Chiefs of Staff. Joint Publication 3-13, *Information Operations.* Washington, DC: Government Printing Office, November 2012.

Kelly, Suzanne. “Government not keeping Pace with Cyber Threats.” *CNN.com*, 1 February 2012. http://security.blogs.cnn.com/2012/02/01/government-not-keeping-pace-with-cyber-threats/ (accessed 30 March 2013).

Kennedy Space Center. “Project Gemini Goals.” 25 August 2000. http://science.ksc.nasa.gov/history/gemini/gemini-goals.txt (accessed 30 September 2013).

——— “Project Mercury Overview.” 26 September 2000. http://www-pao.ksc.nasa.gov/history/mercury/mercury-overview.htm (accessed 30 September 2013).

Knight Ridder Newspapers. “Plan Would Create New Space Force.” *Northwest Florida Daily News*, 26 March 1999. http://search.proquest.com/docview/379432501?accountid=28992 (accessed 3 October 2013).

Mazza, Michael. “Cyberattacks: An Unprecedented Threat to US national Security.” American Enterprise Institute, 21 March 2013. http://www.aei.org/speech/foreign-and-defense-policy/defense/cyber-attacks-an-unprecedented-threat-to-us-national-security/ (accessed 30 March 2013).

McFarland, Stephen L. *A Concise History of the U.S. Air Force*. Washington, DC: Air Force History and Museums Program, 1997. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA433274 (accessed 30 March 2013).

McIlvain, Rob. "Army Sees Cyber Threats as Imminent." The Official Homepage of the United States Army, 28 October 2011. http://www.army.mil/article/68283/ (accessed 30 March 2013).

Mick, Jack. "Chinese Hackers Score F-35, Black Hawk Chopper, and PATRIOT Missile Data." *Daily Tech*, 28 May 2013. http://www.dailytech.com/Chinese+Hackers+Score+F35+Black+Hawk+Chopper+and+PATRIOT+Missile+Data/article31638.htm (accessed 1 November 2013).

Mission and Spacecraft Library. "Defense Satellite Communications System." http://space.jpl.nasa.gov/msl/Programs/dscs.html (accessed 1 October 2013).

Mulrine, Anna. "Cyber Security: The New Arms Race for a New Front Line." *The Christian Science Monitor*, 15 September 2013. http://www.csmonitor.com/USA/Military/2013/0915/Cyber-security-The-new-arms-race-for-a-new-front-line (accessed 3 October 2013).

Murphy, Matt. "Cyberware: War in the Fifth Domain." *The Economist*. 1 July 2010. http://www.economist.com/node/16478792 (accessed 30 March 3013).

Myers, Ryan Todd. "Military Expansion: The Need for a Separate Space Force." Thesis, California State University, Long Beach, 1999. http://search.proquest.com/docview/304595199?accountid=28992 (accessed 3 October 2013).

Nalty, Bernard C. *Winged Shield, Winged Sword: A History of the United States Air Force*. Washington, DC: Air Force History and Museums Program, 1997.

National Aeronautics and Space Administration (NASA). "NASA History in Brief." 20 May 2011. http://history.nasa.gov/brief.html (accessed 30 September 2013).

Olson, Melissa. "History of Laser Weapon Research." Naval Surface Warfare Center, Dahlgren Division, Corporate Communication, 2012. www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA557756 (accessed 1 October 2013).

Poling, Bill. "10 Years: How 9/11 Changed Travel?" *Travel Weekly*, 31 August 2011. http://www.travelweekly.com/travel-news/travel-agent-issues/10-years--how-9/11-changed-travel/ (accessed 30 March 2013).

Putic, George. "Stuxnet: An Effective Cyberwar Weapon." Voice of America, 28 June 2013. http://www.voanews.com/content/stuxnet-an-effective-cyberwar-weapon/1691311.html (accessed 3 October 2013).

Rosenberg, Jennifer. “First Man on the Moon.” About.com Education 20th Century History. http://history1900s.about.com/od/1960s/p/firstmanmoon.htm (accessed 30 September 2013).

Schaff, Marta. “Sputnik & the Space Race.” September 2009. http://web.ebscohost.com/ehost/detail?sid=4d701ff4-5336-4d95-8768-cf867720d04a%40sessionmgr104&vid=1&hid=128&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=khh&AN=18002119 (accessed 30 September 2013).

Shanker, Thom. “Hagel Gives Dire Assessment of Choices He Expects Cuts to Force on the Pentagon.” *New York Times*, 31 July 2013. http://www.nytimes.com/2013/08/01/us/politics/hagel-sees-2-paths-for-cuts-paring-militarys-size-or-capability.html (accessed 4 October 2013).

Space Foundation. “2012 Annual Report.” http://www.spacefoundation.org/docs/SF-2012-annual-report.pdf (accessed 2 October 2013).

Tate, James P. *The Army and Its Air Corps: Army Policy toward Aviation, 1919-1941*. Maxwell Air Force Base: Air University Press, 1998.

U.S. Department of State. “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies.” Bureau of Arms Control, Verification and Compliance. http://www.state.gov/t/isn/5181.htm (accessed 1 October 2013).

U.S. Strategic Command. “U.S. Cyber Command,” Fact Sheets, August 2013. http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 3 October 2013).

White House. “Remarks by the President in the State of the Union Address.” 12 February 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address (accessed 30 March 2013).

Whittington, Michael C. *A Separate Space Force, An 80-Year-Old Argument*. Maxwell Paper No. 20. Maxwell Air Force Base, AL: Air War College, May 2000. www.au.af.mil/au/awc/awcgate/maxwell/mp20.pdf (accessed 3 October 2013).